Montgomery McCracken

Wiretaps and Undercover Sting Operations: Are White Collar Defendants Ready?

By Mark B. Sheppard and Ryan Anderson

"Out are the days of resting easy in the belief that only self-reporting or tipsters will bring criminality to light. In are the days of proactive and innovative white collar enforcement." Lanny Breur, February 25, 2010, at the 24th annual National Institute on White Collar Crime.

I. Introduction

The DOJ has aggressively used proactive enforcement techniques such as undercover sting operations and enhanced use of electronic surveillance in white collar cases. The recent FCPA arrests at a Las Vegas gun show following a two year long sting investigation and the *Galleon* case in New York are but two of the more prominent examples. These techniques, once reserved for drug and organized crime conspiracies are now becoming part of garden variety health care and financial fraud investigations. As a result, white collar practitioners can no longer afford to be in the dark regarding these techniques and the law that surrounds them.

A. FCPA Sting Case

22 defendants, 16 unsealed indictments --- "represent[s] the largest single investigation and prosecution against individuals in the history of DOJ's enforcement of the FCPA." - DOJ release. The indictments, following over two and a half years of sting operations, allege that the 22 defendants allegedly agreed to pay a 20 percent bribe to sales agents supposedly representing the foreign defense minister in return for a $15 million contract. In reality, the sales agent was an undercover FBI agent.

B. Galleon Group

Over 18,000 intercepted recordings through use of informant wearing a wire --- Thousands of wiretaps were made in the criminal investigation between 2003 and 2009. David Slaine, a former hedge fund manager identified as a government "mole" in an undercover sting operation targeting the fallen Galleon Group. Slaine agreed to secretly record conversations used against Galleon after federal authorities caught him trading on inside tips supplied by UBS in a separate case. On March 10, 2010, it was reported that federal prosecutors wired several cooperating witnesses in the Galleon Group insider trading case in order to obtain information on other targets of the investigation.

The wiretapping law jurisprudence that developed in the 1970's has been well settled for decades and practitioners in drug and gang cases are very familiar with this area of the law. White collar practitioners are now confronted with these old tactics in a new forum. White collar defendants are being caught on tape and their attorneys must be prepared to defend against the

tapes. The applicability of the wiretapping laws to white collar cases is new relatively uncharted and as such, presents both concern and opportunity.

II. Defending against Title III Evidence– Federal Wiretap Law

Congress enacted the Federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) in an effort to balance the privacy rights of individuals and the legitimate needs of law enforcement. See United States v. Dalia, 441 U.S. 238, 250 n.9, 252 (1979). The Act seeks to safeguard privacy in oral and wire communications while simultaneously articulating when law enforcement officials may intercept such communications. See Gelbard v. United States, 408 U.S. 41, 48 (1972). Title III prohibits the intentional interception of wire, oral or electronic communications, unless specifically provided for in the statute. 18 U.S.C. § 2511(1).

The strict procedural and evidentiary requirements of the Act, provide plenty of room for creative lawyering. Although courts have been less and less likely to enforce the strict requirements of sealing or having the right official sign the application, rather than just authorize the wiretap, there is still plenty to fight when confronted with wiretap evidence.

A. "Technical" or "Facial" Challenges to a Title III Electronic Interception

1. Challenge Each Wiretap Application and Order Independently, Within its Four Corners

A defense challenge should analyze each separate application (and supporting affidavit) in turn. See, e.g., United States v. Carneiro, 861 F.2d 1171, 1176 (9th Cir. 1988) ("The district court erred in failing to examine each wiretap application separately. Each wiretap application, standing alone, must satisfy the necessity requirement."); U.S. v. Majeed, 2009 WL 2393439, 13 (E.D.Pa. 2009)(showing a thorough wiretap by wiretap analysis.). Moreover, when defending the wiretap applications and orders, the government must be limited to the facts and information contained within the application and affidavits when presented to the authorizing court. See, e.g., United States v. Meling, 47 F.3d 1546, 1551-52 (9th Cir. 1995) ("Looking only to the four corners of the wiretap application, we will uphold the wiretap if there is a substantial basis for these findings of probable cause."). Note, however, that the government can incorporate testimony or affidavits by reference in the application (as long as these documents are physically before the authorizing court).

2. Did the Correct DOJ Official Authorize the Application?

Title III requires that the Attorney General of the Department of Justice, or a properly-designated subordinate, to authorize an AUSA's application for a wiretap. The DOJ official that authorized the wiretap application must be specifically identified in the application. 18USC § 2518(1). Similarly, the ultimate wiretap order must specify the person at DOJ who authorized the application. 18 USC § 2518(4); see also United States v. Reyna, 218 F.3d 1108 (9th Cir. 2000) ("Both the application and the court order approving the application must state the identity of the officer authorizing the application.").

The Title III provisions regarding authorizing officials can be roughly summarized as follows:

Section 2518(10)(a)(iii): Authorizes defense challenges to wiretap orders;

- Section 2518(4)(d): Requires orders to reflect the identity of the authorizing official;
- Section 2516(1): Limits the pool of DOJ officials empowered to authorize an application.

There are an astounding number of cases where the government fumbles this essential step. See, e.g., United States v. Giordano, 416 U.S. 505, 525-26 (1974) (upholding suppression when wiretap application was not approved by designated official, but by Attorney General's Executive Assistant); United States v. Chavez, 416 U.S. 562 (1974) (suppressing wiretap proceeds when application had not been approved by Attorney General or designated Assistant Attorney General); United States v. Traitz, 871 F.3d 368, 379-80 (3rd Cir. 1989) (upholding wiretaps when contested application and order identified the authorizing official by title, but not by name); United States v. Camp, 723 F.2d 741, 744 (9th Cir. 1984) (permitting the Attorney General to designate the Assistant Attorney General by job title rather than name); United States v. Citro, 938 F.2d 1431, 1435 (1st Cir. 1991) (permitting the Attorney General to designate Assistant A.G.'s by title, rather than by name).

3. Sealing Requirements

Title III requires that "[ijmmediately upon the expiration of the period of the order [authorizing wiretapping], or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions." 18 USC § 2518(8)(a). "The government must follow these procedures or it cannot use the intercepted communications against the surveilled individual in a criminal trial. To use wiretap evidence, the government must (1) seal the tapes immediately or (2) provide a 'satisfactory explanation' for the delay in obtaining a seal." United States v. McGuire, 307 F.3d 1192, 1202-03 (9th Cir. 2002) (citing United States v. Pedroni, 958 F.2d 262, 265 (9th Cir. 1992)); See also U.S. v. Quintero, 38 F.3d 1317 (3d Cir. 1994) (hectic trial schedule is the norm for federal prosecutors and is not a satisfactory explanation for failure to seal wiretap tapes immediately).

Therefore, an early task in wiretap litigation is to visit the facility where the original tapes or data was stored, and examine the sealing orders and logs for the data.

4. Minimization Challenges

Title III requires the minimization of calls:

> .... Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or

> foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. 18 USC § 2518(5).

The Third Circuit has advised that "[o]ur inquiry is on the 'reasonableness' of minimization efforts, under the totality of the circumstances." United States v. Hull, 456 F.3d 133, 142 (3d Cir. 2006) (citing Scott, 436 U.S. 128, 140 (1978)). In Scott, the Court found that such circumstances included "the purpose of the wiretap and the information available to the agents at the time of interception." Scott, 436 U.S. at 132-33. See also United States v. Vento, 533 F.2d 838, 854 (3d Cir. 1976) ("Minimization is not to be judged by a rigid hindsight that ignores the problems confronting the officers at the time of the investigation."). Thus, minimization requirements are less stringent where, because of coded language and one-time only calls, "agents can hardly be expected to know that calls are not pertinent prior to their termination." Scott, 436 U.S. at 140.

The Third Circuit further instructs that "[t]he mere number of intercepted, but nonpertinent calls, is not dispositive." Hull, 456 F.3d at 143 (citing to United States v. Adams, 759 F.2d 1099, 1115 (3d Cir. 1985)). In Armocida, where agents intercepted seventy-seven (77) "personal" calls, most of which lasted less than two (2) minutes, the court stated that under the circumstances it would not find "that a full interception of a one-and-one-half minute to two minute conversation violates the minimization requirements." United States v. Armocida, 515 F.2d 49, 52 (3d Cir. 1975).

The Third Circuit has articulated three "crucial" factors for the minimization analysis. Id. at 52-53. First, a court reviewing minimization efforts should consider "the nature and scope of the criminal enterprise under investigation." Id. "[S]omewhat greater latitude may be allowed where conspirators converse in a colloquial code, thereby creating superficially innocent conversations that are actually relevant to the investigation." Id. Moreover, large-scale investigations of criminal conspiracies may need to intercept a greater number of conversations, especially when "the judicially approved wiretap is designed to identify other participants in the conspiracy and to determine the scope of the conspiracy." Id. More recently, the Hull court reiterated that "when investigating a wide-ranging conspiracy between parties known for their penchant for secrecy, broader interceptions may be warranted." Hull, 456 F.3d at 142.

Second, courts should consider "the government's reasonable expectation as to the character of, and the parties to, the conversations." Armocida, 515 F.2d at 44. By way of example, "if the government knows during what time of the day the telephone will be used for criminal activity, it can avoid intercepting calls at other times." Id. The Supreme Court in Scott explained that while agents should not listen to every call over a wiretap on a public telephone where one person is suspected of placing illegal bets, "if the phone is located in the residence of a person who is thought to be the head of a major drug ring, a contrary conclusion may be indicated." Scott, 436 U.S. at 140.

Third, "the degree of judicial supervision by the authorizing judge" must be considered.

Armocida, 515 F.2d at 44. Section 2518(6) of Title III "permits a district judge, once he has authorized a wiretap, to continue supervising the operation of the interception by requiring reports from the government." Id. Such supervision should be taken into consideration when determining the adequacy of the government's minimization efforts. Id. at 44-45.

The minimization argument, however, is a tedious one that is of limited benefit. In United States v. Cox, 462 F.2d 1293, 1302 (8th Cir. 1972), cert. denied, 417 U.S. 918, 94 S.Ct. 2623, 41 L.Ed.2d 223 (1974) the court allowed for the only remedy for failure to minimize wiretapping to be civil suit for the disclosure of the information under § 2520. In United States v. LaGorga, 336 F. Supp. 190, 196 (W.D.Pa. 1971) the court decided that suppression only applies to the specific interception which is determined to be unlawful, rather than a blanket order which would affect all the evidence, including that obtained by procedures sanctioned by statute and Court Order.

B. "Necessity" Shortcomings as a Challenge to Electronic Interceptions

1. Necessity and Normal Investigative Techniques

Title III requires that a wiretap application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 USC § 2518(l)(c).

Similarly, a wiretap order must reflect a determination that the procedure is necessary: "Upon such application the judge may enter an ex parte order … authorizing … interception of … electronic communications … if the judge determines on the basis of the facts submitted by the applicant that … normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 USC § 2518(3)(c)(3).

"The statutory language suggests that before finding that a wiretap is necessary, the court must find that alternative methods have been tried or would not have succeeded." United States v. Ippolito, 774 F.2d 1482, 1485 (9th Cir. 1985). Electronic interceptions should not be permitted if "traditional investigative techniques would suffice to expose the crime." United States v. Kahn, 415 U.S. 143, 153 & n.12 (1974); see also United States v. Williams, 124 F.3d 411, 418 (3d Cir. 1997) and United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975). In order to satisfy this requirement, however, the government need only lay a "factual predicate" sufficient to inform the judge why other methods of investigation are not sufficient. United States v. McGlory, 968 F.2d 309, 345 (3d Cir. 1992).

Although the application for a wiretap is likely to follow the guidance of the courts and reflect that alternative methods have been tried and failed, it is possible through a Franks hearing to show that those methods were exaggerated. See United States v. Ippolito,774 F.2d 1482, 1485 (9th Cir. 1985), wherein the officer did not include that the confidential informant was cooperating in the investigation and willing to testify. After the Franks analysis, it was determined that given an informant who was willing to testify, the necessity requirement was not met.

What normal investigative techniques must be exhausted before the government resorts to a wiretap? Here is a list to explore when examining the sufficiency of the government's investigative efforts before a wire:

- Search warrants
- Witness interviews
- Grand jury testimony/subpoena
- Cooperating witnesses/informants
- Infiltration by undercover agents
- Controlled buys
- Surveillance
- Video surveillance
- Trash covers
- Mail covers
- Financial investigations
- Pen registers
- Toll registers (phone records)
- Trap and trace

See generally S. REP. 90-1097, 1968 U.S.C.C.A.N. 2112, 2190 ("The judgment would involve a consideration of all the facts and circumstances. Normal investigative procedure would include, for example, standard visual or aural surveillance techniques by law enforcement officers, general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants.").

2. Specificity and Boilerplate

Circuit courts have rejected the government's increasing use of boilerplate language in support of its necessity showing. As the Ninth Circuit has explained, the government cannot simply rest on generalizations, but instead, "[M]ust allege specific circumstances that render normal investigative techniques particularly ineffective or the application must be denied ...." Ippolito, F.2d at 1486; see also U.S. v. Teagle, 2007 WL 2972554 (E.D.Pa. 2007).

The government cannot skirt the necessity requirement by simply informing the court of the investigating agents' conclusions regarding whether or not traditional investigative techniques will suffice to expose the crime. Requisite necessity cannot be shown by "bare conclusory statements that normal techniques would be unproductive." United States v. Ashley, 876 F.2d 1069, 1072 (1st Cir. 1989). See also U.S. v. Teagle, 2007 WL 2972554 (E.D.Pa. 2007) at *4 explaining the specificity of an application.

3. Necessity Showings Cannot Be Bootstrapped from Previous Investigations or Applications

The necessity rule is that each wiretap application must stand on its own. Similarly, the government cannot aggregate necessity from other wiretap applications to collectively show necessity for a subsequent application. See United States v. Carneiro, 861 F.2d 1171, 1176 (9th Cir. 1988); U.S. v. Majeed, 2009 WL 2393439, at *11 (E.D.Pa. 2009).

The need for individualized necessity and probable cause showings often is at issue in extension applications. Extension applications are not merely formalities that automatically extend an original wiretap. Section 2518(5) of Title 18 requires that each application for an extension of a wiretap must include a full statement of facts regarding necessity, as is required for original applications under section 2518(l)(c). There is, however, an additional statutory requirement in Title III for extension applications. Section 2518(l)(f) specifically requires an extension affidavit to provide "a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results." 18 USC § 2518(f). Failure to provide adequate necessity for an application means that probable cause is not shown and the wiretap will be suppressed. U.S. v. Majeed, 2009 WL 2393439, at *11 (E.D.Pa. 2009)

The Supreme Court has acknowledged these separate requirements for extension applications. In Giordano, the Court observed that "extension orders do not stand on the same footing as original authorizations … but are provided for separately." Giordano, 416 U.S. at 530. It then emphasized the additional showing required by Section 2518(l)(f). Id. The Court found a common-sense rationale for this greater showing: Plainly the function of § 2518(l)(f) is to permit the court realistically to appraise the probability that relevant conversations will be overheard in the future. If during the initial period, no communications of the kind that had been anticipated had been overheard, the Act requires an adequate explanation for the failure before the necessary findings can be made as a predicate to an extension order. Id.

C. Probable Cause Shortcomings in Wiretap Applications and Orders

1. The Three P.C. Requirements of Title III

A wiretap application (and the resulting order) must establish probable cause in relation to three facts: i) that an individual is committing crime, ii) that communications about that crime will be intercepted, and iii) that the phone line tapped is being used to communicate about the crime. 18 USCA § 2518(3)(a)(b) & (d).

a. Is the Individual Committing a Crime?

As with a traditional search warrant affidavit, a wiretap application must establish that the target has committed or is committing a crime. 18 USC § 2518(3)(a). There are limits as to which crimes are permissible bases for a wiretap (albeit, very broad limits). The statute permits wiretaps for crimes enumerated in 18 USC § 2516. That statute, in turn, provides a laundry list of federal offenses ranging from assassination of the President to obscenity. Id. The classic wiretapping subjects – drugs and guns clearly fall within the statute, as do all acts of fraud, wire fraud, and bank fraud, as well as computer fraud and nearly one-hundred other enumerated offenses. If the wiretap produces unusual charges, it is worth it to check Section 2516 to make sure the crime is enumerated.

b. Will Communications about the Crime be Intercepted?

Before obtaining a wiretap, the government must show probable cause that communications about the crime will be intercepted. 18 USCA § 2518(3)(b).

c. Are there Criminal Communications on the Target Line?

The final probable cause requirement is whether a specific target line (a specific phone number) is being used for criminal conversations. 18 USCA § 2518(3)(d). This is obviously closely related to the second probable cause requirement, that "particular communications" regarding crimes will be intercepted (section 2518(3)(b)).

Both b and c appear to be areas ripe for defending in white collar cases. The chances that white collar defendants will be taking at any particular time about a criminal enterprise, or that a particular line may be fruitful for the investigation would seem hard to prove.

d. Staleness

Staleness is another area where an argument can be made against the wiretap. Staleness, however, is unlikely to work. The Third Circuit Court of Appeals has explained that "where the facts adduced to support probable cause describe a course or pattern of ongoing and continuous criminality, the passage of time between the occurrence of the facts set forth in the affidavit and the submission of the affidavit itself loses significance." United States v. Urban, 404 F.3d 754, 774 (3d Cir. 2005). The Court has further specified that "[t]he liberal examination given staleness in a protracted criminal conduct case 'is even more defensible in wiretap cases than in ordinary warrant cases, since no tangible objects which can be quickly carried off are sought.'" Id. at 775.

D. Franks Challenges to Electronic Interceptions

1. Franks and Title III Challenges

Under the Fourth Amendment, a defendant may challenge a search conducted pursuant to a warrant on the grounds that the warrant affidavit, even though facially adequate to support probable cause, contained factual misstatements or omissions that influenced the issuing magistrate. See Franks v. Delaware, 438 U.S. 154 (1978). If the reviewing court determines that an affiant has knowingly or recklessly included false information that is material to the determination of probable cause, evidence seized pursuant to that warrant must be suppressed. See U.S. v. Majeed, 2009 WL 2393439, at *13 (E.D.Pa. 2009).

This reasoning applies with equal force to wiretap affidavits. United States v. Ippolito, 774 F.2d 1482, 1485 (9th Cir. 1985); Majeed, 2009 WL 2393439, 13 (E.D.Pa. 2009). The Franks legal analysis in the context of a wiretap motion is similar to the Franks approach to a search warrant. One significant difference is the impact of the omissions or misstatements upon the government's application; in a wire motion, a Franks error may jeopardize not only probable cause, but also necessity for the wiretap. See, e.g., Ippolito, 774 F.2d at 1485 ("The necessity showing and finding are therefore material to the issuance of a wiretap order and are subject to Franks").

A defendant seeking a Franks hearing must make a "substantial preliminary showing," Franks, 438 U.S. at 170, that (1) the affidavit contains a material misrepresentation, (2) the affiant made the misrepresentation knowingly and intentionally, or with reckless disregard for the truth, and (3) the allegedly false statement was material to the finding of probable cause. See id. at 155-56, 171; see also United States v. Brown, 3 F.3d 673, 676 (3d Cir. 1993). Where the defendant asserts that the affiant omitted facts with a reckless disregard for the truth, the defendant can satisfy the substantial preliminary showing standard by demonstrating that "an officer recklessly omit[ed] facts that any reasonable person would want to know." United States v. Yusuf, 461 F.3d 374, 383 (3d Cir. 2006) (citing Wilson v. Russo, 212 F.3d 781, 783 (3d Cir. 2000)). If the defendant makes this preliminary showing, but "there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." Id. at 171–172. If "the remaining content is insufficient," then the defendant is entitled to a hearing. Id. at 172.

2. Taint from Previous Wiretaps

If an original wiretap was improvidently granted, the government cannot use the fruits of that wiretap to obtain authorization for later interceptions. See, e.g., United States v. Giordano, 416 U.S. 505, 529-30 (1974) ("Even though suppression of the wire communications intercepted under the October 16, 1970, order is required, the Government nevertheless contends that communications intercepted under the November 6 extension order are admissible because they are not 'evidence derived' from the contents of communications intercepted under the October 16 order within the meaning of § § and 2518(10)(a). This position is untenable."); United States v. Vento, 533 F.2d 838, 847 (3d Cir. 1976) ("If the government's application did not present probable cause for the authorization of the interception, then the authorization and any surveillance pursuant to it were improper. And, if the surveillance was improper, the government could not use the fruits of that surveillance at trial or to further its investigation.").

III. Practical Considerations

A. Early Disclosure of Wiretap Applications and Ten-Day Reports

Title III requires that wiretap applications and orders be disclosed ten days before wiretap proceeds are used in any trial, hearing, or other proceeding in a federal or state court. See 18 USC § 2518(9). Although this was presumably intended for evidentiary hearings and trial, this disclosure provision has also been held to apply to detention hearings. See United States v. Salerno, 794 F.2d 64 (2d Cir. 1986), rev'd on other grounds, 107 S. Ct. 2095 (1987) ("We think it clear that Congress intended § 2518(9) to apply to detention hearings.") Early and aggressive invocation of this right can help back government counsel off of relying on wiretap proceeds in bail hearings (as an AUSA rarely has disclosure ready that early in the case).

B. Early Identification of Cooperating Informants

Wiretaps are expensive and time-consuming, and are typically only used in fairly serious cases. With the corresponding high federal sentencing exposures, the likelihood that co-defendants will flip and become cooperating witnesses increases. It is common for a wiretap application to refer

to cooperating witnesses or informants by code name - and those informants' identities typically will not be disclosed, because they will not be used at trial. Every co-defendant who cooperates early in the case represents a lost opportunity to identify these wire informants.

One of the earliest tasks in a defense against wiretap evidence should therefore be to cull all references to the cooperating wire witnesses and informants, and prepare short and easy-to-read memos listing their characteristics. These memos should be distributed to all defendants, and counsel should aggressively push their clients to try to identify the informants. Delay on this chore can mean that the one defendant who knew a cooperating wire informant may be lost to the lure of a §5K1.1 deal.

C. View the Physical Documents

It pays to be a skeptic in wiretap litigation. For example, in a recent wiretap in the Northern District of California, the government completely failed to attach a referenced affidavit to a wiretap extension application. The application was nonetheless approved. That dramatic omission would have never been detected if someone hadn't gone through all of the hard copy applications and affidavits in the district court clerk's office.

Very close review of the materials actually on file can reveal missing (and essential) attachments, applications that were authorized by the DOJ official after the district court issued the wiretap order, and DOJ authorizations that are missing altogether. It is an essential step in mounting a wiretap challenge.

D. Fight the recordings themselves

1. Interpretation of words and context

The transcripts are nothing but interpretation. Everything on those recordings is open to interpretation. Nobody in the real world speaks in clear prose, with footnotes explaining their jargon and inside references. Nobody talks like that. People throw ideas around. They talk things through. They change their mind. Taken out of context, a statement on Day 1 can sound really incriminating. But in context with a statement on Day 2, it's perfectly innocent. It is critical that the defense listen to all of the intercepts, not just those highlighted by the prosecution. The defense needs to get the whole context, and be able to explain ostensibly incriminating conversations as being perfectly innocent. The client should help as much as possible.

2. Audibility

Nobody enunciates every consonant. Speech is casual and it's rushed and it's muddled. People often hear patterns where they don't exist, and hear words and meanings that were never said. Have an inaudibility hearing if you have to, and get the statement tossed altogether if need be.

3. Practical Advice on obtaining a Franks Hearing

- Obtain a copy of the warrant, application for a warrant with all accompanying affidavits and the inventory.
- Obtain all police reports regarding the issuance and execution of the warrant.
- Give the above to the client and discuss with client.
- Verify all statements in the affidavits and application for warrant.
- Analyze the application and affidavits for omissions.
- Investigate the affidavit and application allegations.
- File motion to suppress with request for Franks hearing.
- Follow through and prove material, deliberate falsehoods or statements made in reckless disregard for the truth (or omissions of material facts) which affect probable cause.
- Submit your own version of a revised affidavit without misstatements and with any omitted material information does not set forth probable cause.
- Argue the revised affidavit fails to support a probable cause finding.
- Confidential informants -
  - obtain their identities
  - get all police reports of statements
  - get prior jail and criminal records
- Obtain prior affidavits and applications in other search warrant cases of the officers.
- Obtain copies of prior convictions of persons named in the application.

An example of Successful Wiretap Franks Application

- United States v. Novaton, 271 F.3d 968 (11th Cir. 2001) (Affidavit for wiretap falsely stated that four informants had been reliable in the past and failed to include statements about the animosity between informants and target).

IV. The Future – FCPA Applied to Pharmaceuticals

A. The possibilities of fake doctors or fake sales representatives conducting sting operations in order to ensnare one another are not so unrealistic. Given state run health care systems, the range of foreign officials covered by the FCPA are substantial. In some countries the entire health care system may involve "foreign official[s]" under the FCPA.

B. In Assistant Attorney General Lanny A. Breuer's November 12, 2009 address to Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum he stated that the DOJ is meshing resources in the Fraud Section's health care and FCPA silos, and department officials said they have met with overseas counterparts to coordinate for their cooperation in the effort.

C. Said Breuer:

> In the pharmaceutical context, we have additional expertise that significantly enhances our ability to proactively investigate and prosecute these often complex cases. That additional expertise is located in our health care fraud group, where we have prosecutors and analysts with the industry knowledge necessary to quickly

> identify corrupt practices. These two groups – our FCPA unit and our health care fraud unit – are already beginning to work together to investigate FCPA violations in the pharmaceutical and device industries in an effort to maximize our ability to effectively enforce the law in this area

V. Conclusion

The expansion of surveillance and sting operations into new areas of criminality reflects a shift in resources and attitudes toward white collar crime. As the DOJ melds the expertise it has in prosecution of these cases, the defense bar must step up its game to properly defend these types of cases. By melding expertise in handling government investigations into corporate practices with experience in defending against overbroad and illegal wiretaps we can provide the best defenses available for our clients.